

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<https://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

09/26/2019

SUBJECT:

A Vulnerability in LibreOffice Could Allow for Arbitrary Command Execution

OVERVIEW:

A vulnerability has been discovered in LibreOffice, which could allow for arbitrary command execution. LibreOffice is an open-source office suite providing word processing, slides, and spreadsheets. Successful exploitation of this vulnerability will enable the attacker to perform command execution in the context of the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There is proof-of-concept code available for this vulnerability.

SYSTEMS AFFECTED:

- LibreOffice 6.2 versions prior to 6.2.7
- LibreOffice 6.3 versions prior to 6.3.1

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in LibreOffice, which could allow for arbitrary command execution. LibreOffice is typically bundled with LibreLogo, a programmable turtle vector graphics script, which can execute arbitrary python commands contained within the document it is launched from. Protection was added to block calling LibreLogo from script event handlers, however a Windows 8.3 path equivalence handling flaw left LibreOffice vulnerable to documents executing LibreLogo via a Windows filename pseudonym. Successful exploitation of this vulnerability will enable the attacker to perform command execution in the context of the user running the affected application. Depending on the privileges associated with the user, an

attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMENDATIONS:

The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by LibreOffice to vulnerable systems immediately after appropriate testing
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9855>

The Document Foundation:

<https://www.libreoffice.org/about-us/security/advisories/cve-2019-9855/>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<https://www.us-cert.gov/tlp/>

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts

Security Operations Analyst

MS Department of Information Technology Services

601-432-8201 | www.its.ms.gov





DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited